(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020030021339 A
(43)Date of publication of application: 15.03.2003

(21)Application number: 1020010054399
(22)Date of filing: 05.09.2001

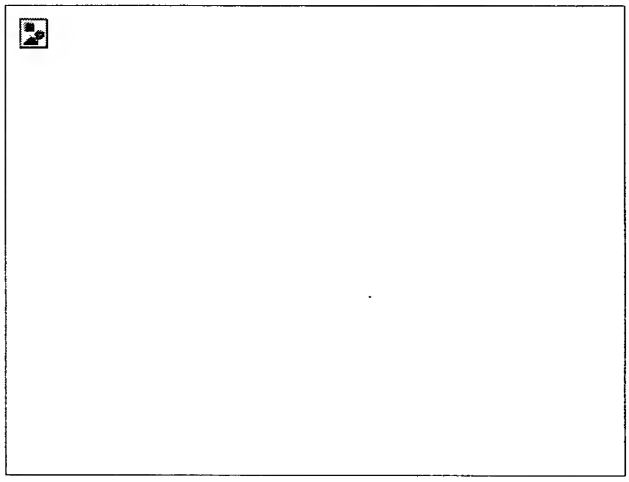
(71)Applicant: ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE
(72)Inventor: JANG, JONG SU
PARK, SANG GIL
SON, SEUNG WON

(51)Int. Cl H04L 12/22

(54) SECURITY GATEWAY DEVICE FOR POLICY-BASED NETWORK SECURITY CONTROL AND OPERATING METHOD THEREFOR

(57) Abstract:

PURPOSE: A security gateway device for a policy-based network security control and an operating method therefor are provided to dynamically meet a cyber terror by updating a correspondence policy according to a terror type in a policy cache when the cyber terror is generated and applying the updated policy to a newly generated cyber terror.



CONSTITUTION: A CPA(Cyber Patrol Agent)(201) receives a cyber terror detection signal, and transmits the received cyber terror detection signal to a CPCS(Cyber Patrol Control System)(300). A policy receiving unit(202) receives a policy corresponding to the cyber terror detection signal from the CPCS(300). A security policy engine(203) receives the policies from the policy receiving unit(202), and outputs a dynamic security policy among the policies. A QoS (Quality of Service) policy executing engine(206) receives the policies from the policy receiving unit(202), and outputs a dynamic QoS policy among the policies. A security policy cache(204) receives the dynamic security policy from the security policy engine(203), and stores the received dynamic security policy according to the type of a cyber terror by a schema unit. A policy cache(205) receives the dynamic security policy of the schema unit from the security policy cache(204), receives the dynamic QoS policy from the QoS policy executing engine(206), updates policy information, and outputs updated policy information to the policy receiving unit(202) for dynamically corresponding to the cyber terror.

Legal Status
Date of final disposal of an application (20040225)
Patent registration number (1004228070000)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04L 12/22

(11) 공개번호 특2003-0021339
(43) 공개일자 2003년03월15일

(21) 출원번호 10-2001-0054399
(22) 출원일자 2001년09월05일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자 박상길
광주광역시북구오치1동940-1번지오치상설시장아파트812호
장종수
대전광역시유성구전민동엑스포아파트303동903호
손승원
대전광역시유성구전민동엑스포아파트208-902
(74) 대리인 특허법인 신성

심사청구 : 있음

(54) 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치및 그 동작 방법

요약

본 발명은 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치 및 그의 동작방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이며, 상기 보안 게이트웨이 장치에 있어서, 사이버 테러 탐지신호를 수신하여, 탐지된 신호를 사이버 순찰 제어 시스템으로 송신하는 사이버 테러 탐지수단; 상기 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 수신하기 위한 정책 수신수단; 상기 정책 수신수단으로부터 정책을 입력받아, 정책 중 동적 보안정책을 출력하기 위한 보안정책 수행수단; 상기 정책 수신수단으로부터 정책을 입력받아, 정책 중 동적 서비스품질(QoS) 정책을 출력하기 위한 서비스품질 정책 수행수단; 상기 보안정책 수행수단으로부터 동적 보안정책을 입력받아, 사이버 테러의 유형에 따라 스키마 단위로 저장하기 위한 보안정책 저장수단; 및 상기 보안정책 저장수단으로부터 스키마 단위의 동적 보안정책을 입력받고, 상기 서비스품질 정책 수행수단으로부터 동적 서비스품질 정책을 입력받아, 정책정보를 업데이트 시켜 상기 정책 수신수단에 출력함으로써, 이후 사이버 테러에 대해 동적으로 대응하기 위한 정책 저장수단을 포함하며, 보안 시스템 등에 이용됨.

대표도

도2

색인어

보안정책, 네트워크, 보안 게이트웨이, 사이버 순찰 제어 시스템

명세서

도면의 간단한 설명

도 1 은 본 발명에 따른 보안 게이트웨이 장치와 전체 보안망과의 연동을 설명하기 위한 전체 보안 시스템의 일실시예 구성도,

도 2 는 본 발명에 따른 보안 게이트웨이 장치의 일실시예 구성도,

도 3 은 본 발명에 따른 보안 게이트웨이 장치의 동작 방법에 대한 일실시예 흐름도.

* 도면의 주요 부분에 대한 부호의 설명

200 : 보안 게이트웨이 201 : 사이버 테러 탐지부

202 : 정책 수신부 203 : 보안정책 수행엔진
204 : 보안정책 캐쉬 205 : 정책 캐쉬
206 : 서비스품질 수행엔진 207 : 정책신호 변환부
300 : 사이버 순찰 제어 시스템 400 : 사이버 테러 대응장치
500 : 보안성 경로 제어장치

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 인터넷 등과 같은 정보통신망의 보안제어 기술분야에 관한 것으로, 더욱 상세하게는 사이버 테러 발생시 테러유형에 따른 대응정책을 보안 게이트웨이 장치 내부의 정책캐쉬에 업데이트시켜, 이후 발생하는 사이버 테러에 대해 상기 업데이트된 정책을 적용함으로써 사이버 테러에 동적으로 대처하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치 및 그 동작 방법과, 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

일반적으로, 해킹에 대하여 학계 및 보안업체에서는 침입 차단 시스템(Firewall), 침입 탐지 시스템(IDS : Intrusion Detection System), 가상 사설망(VPN : Virtual Private Network) 등의 기술을 이용하여 대처하고 있다.

침입 차단 시스템(Firewall)은 주로 패킷 필터링(Packet Filtering)이나 IP(Internet Protocol) 주소를 기반으로 외부 네트워크로부터의 접속을 차단하는 시스템으로서, 외부의 허가되지 않은 패킷에 대해서 내부 시스템으로의 접근을 봉쇄하지만 정책에 의해 허가받은 패킷은 내부 시스템으로의 접근이 자유로우므로 정책에 의해 허용된 사용자나 서비스의 불법적인 변용에 대하여 대처하지 못할 뿐만 아니라, 내부 사용자들의 불법적인 행동들을 차단할 수 없는 문제점이 있었다.

전통적으로 보안 게이트웨이는 근거리통신망(LAN : Local Area Network) 규모의 네트워크 보안을 위해 패킷 필터링을 위한 방화벽 및 가상 사설망(VPN : Virtual Private Network) 구축을 위한 가상 사설망 서버 중심으로 개발되어 왔으며, 새롭게 개발된 해킹방법으로 망에 침입하였을 때, 그 때마다 사람에 의해 정책이 다시 업데이트 되고 각 보안도구(침입 차단 시스템, 침입 탐지 시스템 등)에 해당 정책이 새롭게 적용되어야 하는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

본 발명은, 상기한 바와 같은 종래의 문제점을 해결하기 위하여 제안된 것으로, 사이버 테러 발생시 테러유형에 따른 대응정책을 보안 게이트웨이 장치 내부의 정책캐쉬에 업데이트 시켜, 이후 발생하는 사이버 테러에 대해 상기 업데이트된 정책을 적용함으로써 사이버 테러에 동적으로 대처하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치 및 그 방법과, 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

즉, 본 발명에서 제시하는 보안 게이트웨이 장치에 탑재되는 사이버 테러 탐지부의 일실시예인 사이버 순찰 에이전트(CPA : Cyber Patrol Agent)를 통하여 네트워크 종단으로부터 사이버 테러 탐지신호가 중앙의 사이버 순찰 제어 시스템(CPCS : Cyber Patrol Control System)에 보고되고, 사이버 순찰 제어 시스템의 단말기에서 관리자에 의해 새롭게 정의되는 정책정보와 각각의 보안 게이트웨이 장치 내부에서 각각의 사이버 순찰 제어 시스템이 공유하고 있는 업데이트된 정책정보를 보안 게이트웨이가 할당받아, 할당받은 정책정보에 의해 사이버 테러에 대응하게 된다.

이러한 사이버 테러에 대한 정책 전달과, 사이버 테러의 보고를 무리없이 제공하기 위해서는 정책을 정의하는 CPCS와 보안 게이트웨이와의 보안성 있는 통신을 제공하는 절차가 필요하며, 사이버 순찰 에이전트가 사이버 테러를 탐지하고 중앙의 정책 매니저에게 통보하는 절차가 필요하다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여 본 발명에 따른 보안 게이트웨이 장치는; 사이버 테러 탐지신호를 수신하여, 탐지된 신호를 사이버 순찰 제어 시스템으로 송신하는 사이버 테러 탐지수단; 상기 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 수신하기 위한 정책 수신수단; 상기 정책 수신수단으로부터 정책을 입력받아, 정책 중 동적 보안정책을 출력하기 위한 보안정책 수행수단; 상기 정책 수신수단으로부터 정책을 입력받아, 정책 중 동적 서비스품질(QoS) 정책을 출력하기 위한 서비스품질 정책 수행수단; 상기 보안정책 수행수단으로부터 동적 보안정책을 입력받아, 사이버 테러의 유형에 따라 스키마 단위로 저장하기 위한 보안정책 저장수단; 및 상기 보안정책 저장수단으로부터 스키마 단위의 동적 보안정책을 입력받고, 상기 서비스품질 정책 수행수단으로부터 동적 서비스품질 정책을 입력받아, 정책정보를 업데이트 시켜 상기 정책 수신수단에 출력함으로써, 이후 사이버 테러에 대해 동적으로 대응하기 위한 정책 저장수단을 포함하여 이루어진 것을 특징으로 한다.

또한, 본 발명은 상기 보안정책 수행수단으로부터 동적 보안정책을 입력받고, 상기 서비스품질 정책 수행수단으로부터 동적 서비스품질 정책을 입력받아, 사이버 테러에 즉시 대응할 수 있도록 상기 사이버 테러

처리 장치에서 인식할 수 있는 정책 신호로 변환하여 출력하는 정책신호 변환수단을 더 포함하여 이루어진 것을 특징으로 한다.

또한, 본 발명은 상기 정책신호 변환수단으로부터 변환된 정책신호를 입력받아, 경보신호를 발생시키거나 세션(Session)을 차단하여 공격자를 보안 게이트웨이로부터 단절시키기 위한 사이버 테러 대응수단을 더 포함하여 이루어진 것을 특징으로 한다.

또한, 본 발명은 상기 정책신호 변환수단으로부터 변환된 정책신호를 입력받아, 보안성 경로를 제공하기 위한 보안성 경로 제어수단을 더 포함하여 이루어진 것을 특징으로 한다.

상기 목적을 달성하기 위한 본 발명은, 정책기반 네트워크 보안제어를 위한 보안 게이트웨이의 동작 방법에 있어서, 사이버 테러를 탐지하여, 탐지된 신호를 사이버 순찰 제어 시스템으로 송신하는 제 1 단계; 상기 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 입력받아, 동적 보안정책과 동적 서비스품질 정책을 추출하여, 기 저장된 사이버 테러별 정책을 갱신하는 제 2 단계; 및 상기 제 2 단계에서 사이버 테러별로 갱신된 정책을 이후 사이버 테러 발생시 보안 게이트웨이장치의 정책 수신부에 출력함으로써, 이후 사이버 테러에 동적으로 대응하는 제 3 단계를 포함하여 이루어진 것을 특징으로 한다.

상기 목적을 달성하기 위한 본 발명은, 프로세서를 구비한 보안 게이트웨이 장치에, 사이버 테러를 탐지하여, 탐지된 신호를 사이버 순찰 제어 시스템으로 송신하는 제 1 기능; 상기 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 입력받아, 동적 보안정책과 동적 서비스품질 정책을 추출하여, 기 저장된 사이버 테러별 정책을 갱신하는 제 2 기능; 상기 제 2 기능에서 사이버 테러별로 갱신된 정책을 이후 사이버 테러 발생시 보안 게이트웨이장치의 정책 수신부에 출력함으로써, 이후 사이버 테러에 동적으로 대응하는 제 3 기능; 상기 제 2 기능에서 추출된 동적 보안정책과 동적 서비스품질 정책을 입력받아, 이 후 사이버 테러에 즉시 대응할 수 있도록 상기 사이버 테러 처리 장치(사이버 테러 대응장치와 보안성경로 제어장치를 통칭함)에서 인식할 수 있는 정책 신호로 변환하는 제 4 기능; 상기 제 4 기능에 의해 변환된 정책신호를 입력받아, 사이버 테러 대응장치가 경보신호를 발생시키거나 세션(Session)을 차단하며, 공격자를 보안 게이트웨이로부터 단절시키는 제 5 기능; 및 상기 제 4 기능에 의해 변환된 정책신호를 입력받아, 보안성경로 제어장치가 보안성 경로를 제공하는 제 6 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

본 발명은 인터넷 망의 침입자들에 의한 공격에 대한 종합적인 광역 사이버 순찰 관리 시스템 중 서브 네트워크의 종단점(진입, 진출)에 설치하는 보안 게이트웨이에 관한 것으로서, 망의 액세스 포인트에 위치하는 보안 게이트웨이내의 사이버 순찰 에이전트 기능을 이용하여 네트워크에 대한 침입을 탐지하고, 보안 게이트웨이에 탑재된 정책기반 침입 방어 메커니즘에 의해 침입방어가 이루어진다.

보안 게이트웨이에서 수행되는 침입 방어 메커니즘은 해킹 유형에 따라 서로 다른 대응 방안을 제공하며, 이는 망의 보안 정책에 따라 제어된다. 이를 위해, 보안 게이트웨이와 중앙의 사이버 순찰 제어 시스템(CPCS)간에는 보안성을 가지는 연결을 통하여 자료를 주고받아야 한다.

상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

도 1 은 본 발명에 따른 보안 게이트웨이 장치와 전체 보안망과의 연동을 설명하기 위한 전체 보안 시스템의 일실시예 구성도이다.

사이버 순찰 제어 시스템(300)은 정책 정의부로서의 역할을 담당하며, 보안 게이트웨이 장치(200)는 정책 시행부로서의 기능을 담당한다.

각 사이버 순찰 제어 시스템(300)은 서로간의 정책정보를 보안 게이트웨이(200)의 정책 캐쉬에 저장하고, 해당 정보를 사이버 테러가 발생되는 보안 게이트웨이(200)에 적용한다.

타겟(Target)(100)에서 사이버 테러가 발생하여 중앙의 사이버 순찰 제어 시스템(CPCS)(300-2)에 보안 위규사항이 통보되면, 사이버 순찰 제어 시스템(300-2)은 보안 위규사항을 참조하여 위규사항의 유무를 체크한 후, 보안 게이트웨이(200-1, 200-2)에 해당되는 정책을 시행하도록 한다.

도 2 는 본 발명에 따른 보안 게이트웨이 장치의 일실시예 구성도이다.

도 2에 도시된 바와 같이, 보안 게이트웨이 장치는 사이버 순찰 에이전트(201), 정책 수신부(202), 보안정책 수행엔진(203), 보안정책 캐쉬(204), 정책캐쉬(205), 서비스품질 수행엔진(206), 그리고 정책신호 변환부(207)를 포함한다.

사이버 테러 대응장치(400)와 보안성 경로 제어장치(500)는 상기 보안 게이트웨이 장치(200)와 독립된 별개의 장치로서 구동될 수 있으며, 도 2 또한 그러한 일실시예를 도시하고 있으나, 사이버 테러 대응장치(400)와 보안성 경로 제어장치(500)는 보안 게이트웨이 장치 내부에 탑재되어 보안 게이트웨이 장치의 일부로서 구동될 수도 있음은 자명하다.

최초, 사이버 테러가 발생하게 되면, 사이버 테러를 탐지하는 사이버 순찰 에이전트(201)에서 이를 탐지하여 탐지정보를 중앙의 사이버 순찰 제어 시스템(300)에 실시간으로 통보하게 된다.

사이버 순찰 제어 시스템(300)이 정의하여 다운로드 하여 주는 정책은 정책 수신부(202)에서 수신하게 되며, 보안정책 수행 엔진(203)은 정책 수신부(202)로부터 보안정책을 추출하여 사이버 테러 대응장치(400) 또는 보안성 경로 제어장치(500)에서 인식할 수 있는 정책신호로 변환하기 위하여 정책신호 변환부(207)로 출력하고, 또한 보안정책을 저장하는 보안정책 캐쉬(204)로 출력한다.

이후, 보안정책 캐쉬(204)는 보안정책 수행 엔진(203)으로부터 보안정책을 입력받아, 사이버 테러의 유형에 따라 분류하여 스키마 단위로 임시 저장하며, 임시 저장한 유형별 보안정책 정보를 저장하는 정책 캐쉬(205)에 출력한다.

여기서, 정책 캐쉬(205)는 기존의 이미 보유하고 있던 정책정보에 보안정책캐쉬(204)로부터 입력받은 유형별 정책정보를 업데이트시킨 후, 이후 사이버 테러 발생시 업데이트된 정책정보를 정책 수신부(202)로 출력함으로써 보안 게이트웨이 장치(200)가 동적으로 사이버 테러에 대응하게 한다.

서비스품질(QoS : Quality of Service) 수행 엔진(205)은 정책 수신부(202)로부터 서비스품질 정책을 추출하여, 보안정책 수행 엔진(203)에서 추출한 보안정책과 함께 정책신호 변환부(207)로 출력하며, 정책신호 변환부(207)는 외부의 사이버 테러 대응장치(400) 또는 보안성 경로 제어장치(500) 등에서 인식할 수 있는 정책 신호로 변환하여 정책정보를 출력한다.

마지막으로, 사이버 테러 대응장치(400)는 정책신호 변환부(207)로부터 변환된 정책신호를 입력받아 경보신호를 발생시키거나 세션(Session)을 차단하여 공격자를 보안 게이트웨이(200)로부터 단절시키며, 보안성 경로 제어장치(500)는 정책신호 변환부(207)로부터 변환된 정책신호를 입력받아 보안성 경로를 제공한다.

도 3 은 본 발명에 따른 보안 게이트웨이 장치의 동작 방법에 대한 일실시예 흐름도이다.

최초, 사이버 순찰 에이전트에서 사이버 테러정보를 탐지하여(301), 탐지된 신호를 사이버 순찰 제어 시스템에 송신하며(302), 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 정책 수신부에서 수신한다(303).

이어서, 정책정보 중 보안정책과 서비스품질 정책을 각각 추출하여(304,305) 추출된 보안정책은 사이버 테러 유형별로 구분하여 스키마 단위로 보안정책 캐쉬에 저장하며(306), 스키마 단위로 분류된 보안정책은 추출된 서비스품질 정책과 함께 정책캐쉬에 출력되어 기존의 정책정보를 업데이트한다(307).

정책캐쉬에 업데이트된 정책정보는 이후 사이버 테러 발생시 정책 수신부(202)로 출력되어 동적으로 대응하게 된다(308).

상기 '304' 단계 및 '305' 단계에서 추출된 정책정보는 사이버 테러 대응장치 또는 보안성 경로 제어장치에서 인식할 수 있는 정책정보로 변환되고(309), 경보신호를 발생시키거나 세션(Session)을 차단하여 공격자를 보안 게이트웨이 장치로부터 단절시키거나 보안성 경로를 제공하는 데 이용된다(310).

상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 롬, 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.

이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형, 및 변경이 가능하다는 것이 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다.

발명의 효과

상기한 바와 같은 본 발명은, 사이버 테러가 발생하였을 때, 보안 게이트웨이를 통하여 사이버 순찰 제어 시스템에 사이버 테러에 대한 정보를 전달하고, 또한 이러한 사이버 테러 정보는 정책에 반영되어 이후 발생되는 사이버 테러에 대하여 업데이트된 보안정책에 따라 보안 게이트웨이 장치가 대응을 하도록 근본적인 대비책을 마련하며, 사람에 의해 매번 정책을 설정하는 번거러움 없이 중앙에서 정의되는 정책에 의해 하부 네트워크의 보안 게이트웨이에 정책을 할당하여 해당 도메인이 하나의 보안 정책 하에 동작하도록 하는 효과가 있다.

(57) 청구의 범위

청구항 1

정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치에 있어서,

사이버 테러 탐지신호를 수신하며, 탐지된 신호를 사이버 순찰 제어 시스템으로 송신하는 사이버 테러 탐지수단;

상기 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 수신하기 위한 정책 수신수단;

상기 정책 수신수단으로부터 정책을 입력받아, 상기 정책 중 동적 보안정책을 출력하기 위한 보안정책 수행수단;

상기 정책 수신수단으로부터 정책을 입력받아, 상기 정책 중 동적 서비스품질(QoS) 정책을 출력하기 위한 서비스품질 정책 수행수단;

상기 보안정책 수행수단으로부터 동적 보안정책을 입력받아, 사이버 테러의 유형에 따라 스키마 단위로 저장하기 위한 보안정책 저장수단; 및

상기 보안정책 저장수단으로부터 스키마 단위의 동적 보안정책을 입력받고, 상기 서비스품질 정책 수행수단으로부터 동적 서비스품질 정책을 입력받아, 정책정보를 업데이트 시켜 상기 정책 수신수단에 출력함으로써, 이후 사이버 테러에 대해 동적으로 대응하기 위한 정책 저장수단

을 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치.

청구항 2

제 1 항에 있어서,

상기 보안정책 수행수단으로부터 동적 보안정책을 입력받고, 상기 서비스품질 정책 수행수단으로부터 동적 서비스품질 정책을 입력받아, 사이버 테러에 즉시 대응할 수 있도록 하기 위하여 사이버 테러 처리 장치(사이버 테러 대응장치와 보안성 경로 제어장치를 통칭함)에서 인식할 수 있는 정책 신호로 변환하여 출력하기 위한 정책신호 변환수단

을 더 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 정책신호 변환수단으로부터 변환된 정책신호를 입력받아, 경보신호를 발생시키거나 세션(Session)을 차단하여 공격자를 보안 게이트웨이로부터 단절시키기 위한 사이버 테러 대응수단

을 더 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치.

청구항 4

제 1 항 또는 제 2 항에 있어서,

상기 정책신호 변환수단으로부터 변환된 정책신호를 입력받아, 보안성이 있는 경로를 제공하기 위한 보안성 경로 제어수단

을 더 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치.

청구항 5

정책기반 네트워크 보안제어를 위한 보안 게이트웨이의 동작 방법에 있어서,

사이버 테러를 탐지하여, 탐지된 신호를 사이버 순찰 제어 시스템으로 송신하는 제 1 단계;

상기 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 입력받아, 동적 보안정책과 동적 서비스품질 정책을 추출하여, 기 저장된 사이버 테러별 정책을 갱신하는 제 2 단계; 및

상기 제 2 단계에서 사이버 테러별로 갱신된 정책을 이후 사이버 테러 발생시 보안 게이트웨이장치의 정책 수신부에 출력함으로써, 이후 사이버 테러에 동적으로 대응하는 제 3 단계

를 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치의 동작 방법.

청구항 6

제 5 항에 있어서,

상기 제 2 단계는,

상기 사이버 순찰 제어 시스템으로부터 상기 사이버 테러 탐지 신호에 대응하는 정책을 정책 수신부에서 수신하는 제 4 단계;

상기 제 4 단계에서 상기 정책 수신부에 수신된 상기 정책을 입력받아, 상기 정책 중 동적 보안정책을 추출하는 제 5 단계;

상기 제 5 단계에서 추출한 상기 동적 보안정책을 보안정책 캐쉬에 사이버 테러 유형별로 스키마 단위로 저장하는 제 6 단계;

상기 제 4 단계에서 상기 정책 수신부에 수신된 상기 정책을 입력받아, 상기 정책 중 동적 서비스품질 정책을 추출하는 제 7 단계; 및

상기 제 6 단계에서 상기 스키마 단위로 저장된 동적 보안정책과, 상기 제 7 단계에서 추출된 동적 서비스품질 정책을 입력받아, 정책캐쉬내의 정책정보를 업데이트하는 제 8 단계

를 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치의 동작 방법.

청구항 7

제 6 항에 있어서,

상기 제 5 단계에서 추출한 동적 보안정책과 상기 제 7 단계에서 추출한 동적 서비스품질 정책을 입력받아, 사이버 테러에 즉시 대응할 수 있도록 상기 사이버 테러 처리 장치에서 인식할 수 있는 정책 신호로 변환하는 제 9 단계

를 더 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치의 동작 방법.

청구항 8

제 7 항에 있어서,

상기 제 9 단계에서 변환된 정책신호를 입력받아, 상기 사이버 테러 대응장치가 경보신호를 발생시키거나 세션(Session)을 차단하여, 공격자를 보안 게이트웨이로부터 단절시키는 제 10 단계

를 더 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치의 동작 방법.

청구항 9

제 7 항 또는 제 8 항에 있어서,

상기 제 9 단계에서 변환된 정책신호를 입력받아, 상기 보안성경로 제어장치가 보안성 경로를 제공하는 제 11 단계

를 더 포함하는 정책기반 네트워크 보안제어를 위한 보안 게이트웨이 장치의 동작 방법.

청구항 10

프로세서를 구비한 보안 게이트웨이 장치에,

사이버 테러를 탐지하여, 탐지된 신호를 사이버 순찰 제어 시스템으로 송신하는 제 1 기능;

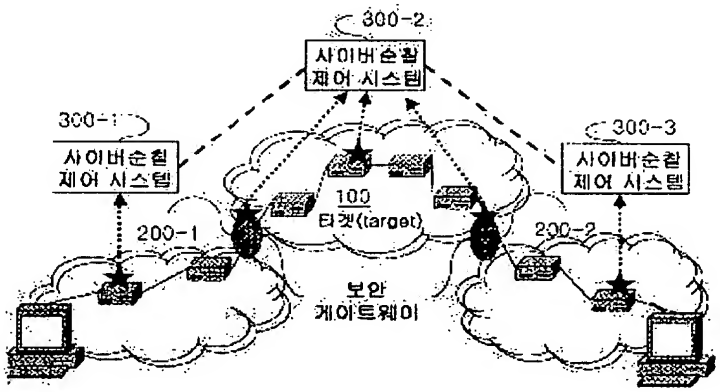
상기 사이버 순찰 제어 시스템으로부터 사이버 테러 탐지 신호에 대응하는 정책을 입력받아, 동적 보안정책과 동적 서비스품질 정책을 추출하여, 기 저장된 사이버 테러별 정책을 갱신하는 제 2 기능; 및

상기 제 2 기능에서 사이버 테러별로 갱신된 정책을 이후 사이버 테러 발생시 보안 게이트웨이장치의 정책 수신부에 출력함으로써, 이후 사이버 테러에 동적으로 대응하는 제 3 기능

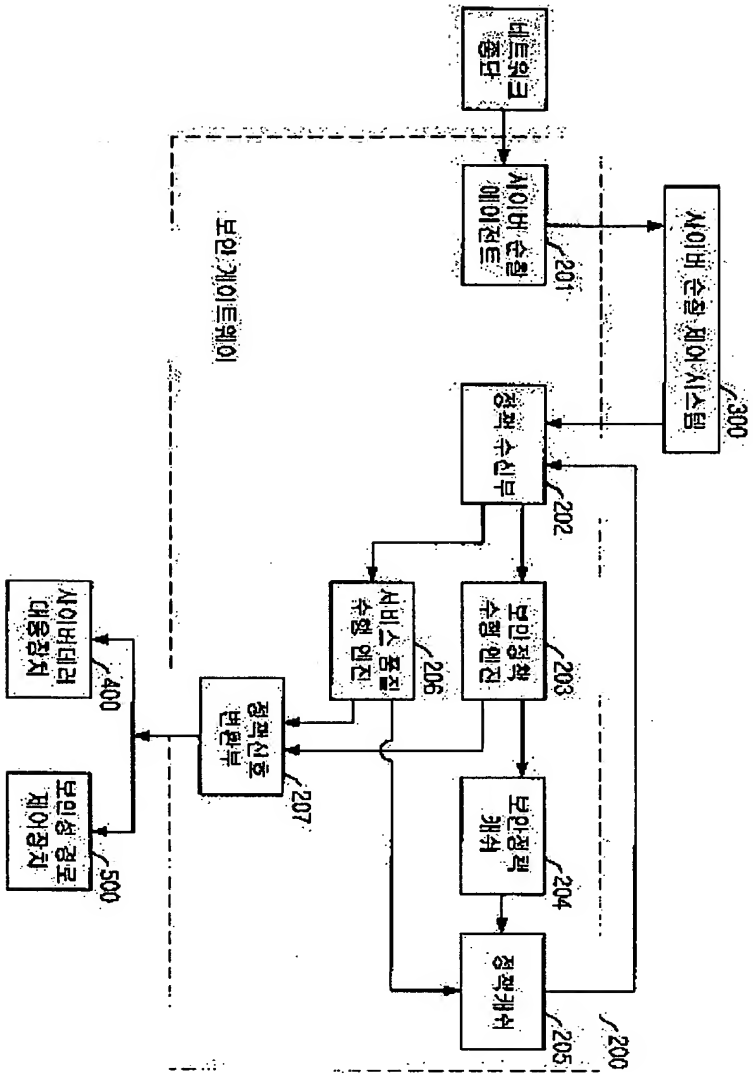
을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

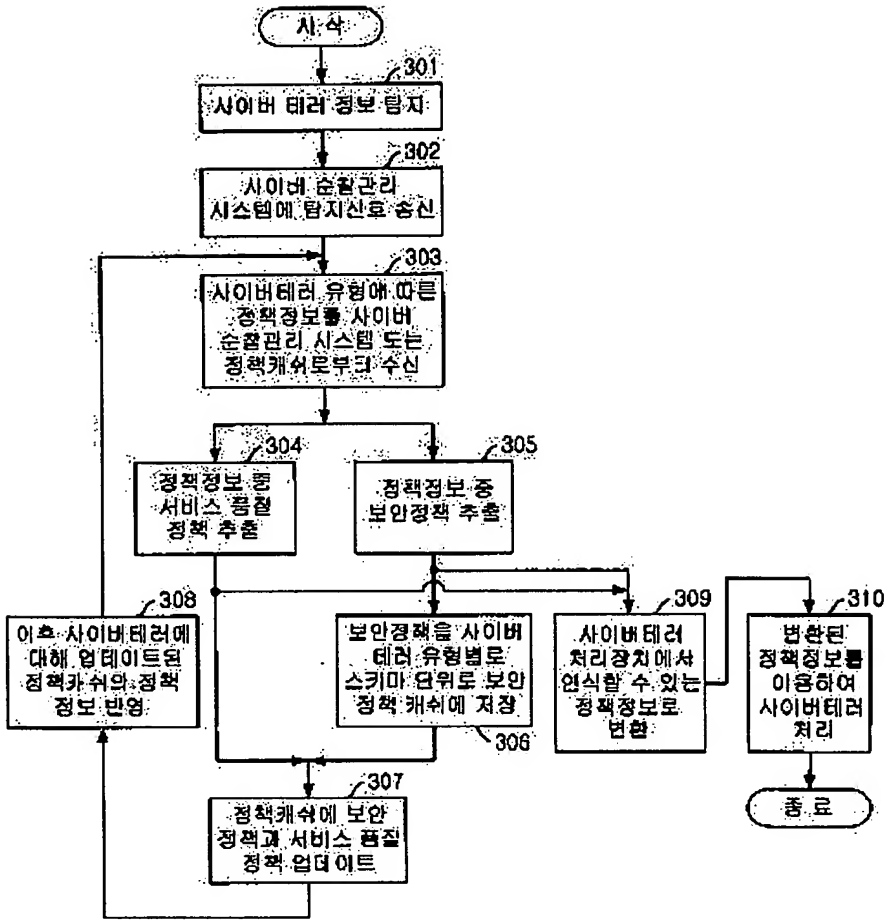
도면1



도면2


네트워크 통보
사이버 순찰 에이전트
201
사이버 순찰 제어 시스템
300
보안 게이트웨이
정책 수신부
202
서비스 품질 수집 엔진
206
보안정책 수집 엔진
203
사이버테러 대응장치
400
정책신호 변환부
207
보안정책 캐쉬
204
보안성 경로 제어장치
500
정책캐쉬
205
200

도면3


시작
301
사이버 테러 정보 탐지
302
사이버 순찰관리 시스템에 탐지신호 송신
303
사이버테러 유형에 따른 정책정보를 사이버 순찰관리 시스템 또는 정책캐쉬로부터 수신
304
정책정보 중 서비스 품질 정책 추출
305
정책정보 중 보안정책 추출
308
이후 사이버테러에 대해 업데이트된 정책캐쉬의 정책 정보 반영
보안정책을 사이버 테러 유형별로 스키마 단위로 보안 정책 캐쉬에 저장
306
309
사이버테러 처리장치에서 인식할 수 있는 정책정보로 변환
310
변환된 정책정보를 이용하여 사이버테러 처리
307
정책캐쉬에 보안 정책과 서비스 품질 정책 업데이트
종료